Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 06 juin 2014
N° CERTFR-2014-ACT-023

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-023

1 - Publication du guide concernant les bonnes pratiques pour l'acquisition et l'exploitation des noms de domaine.

La semaine dernière, l'ANSSI a publié un guide sur les bonnes pratiques pour l'acquisition et l'exploitation des noms de domaine. Ce guide s'adresse potentiellement à toute entité ayant une présence sur internet.

Le protocole DNS (« Domain Name System ») a pour objectif d'associer un nom de domaine mémorisable par un utilisateur à une adresse IP. La gestion de ces noms de domaine doit se faire en respectant certaines règles de sécurité. En effet, leurs compromissions peuvent entraîner l'interception de trafic et de courriers électroniques, des hameçonnages, des dénis de service, ou encore des défigurations de sites web.

Ce guide a pour but de présenter :

- les vulnérabilités du protocole DNS ;
- les différents acteurs impliqués dans l'enregistrement d'un nom de domaine ainsi que leurs rôles ;
- les aspects techniques de la mise œuvre d'une infrastructure de gestion de noms de domaine ;
- les aspects juridiques liés à l'acquisition d'un nom de domaine.

Le CERT-FR recommande aux entités possédant un nom de domaine de tester la configuration de leurs serveurs DNS (en utilisant par exemple ZoneCheck) et mettre en œuvre les préconisations de ce guide.

Documentation

- Guide sur les bonnes pratiques pour l'acquisition et l'exploitation des noms de domaine :
  http://www.ssi.gouv.fr/IMG/pdf/guide_dns_anssi.pdf
- Test de la configuration DNS avec zonecheck :
  http://www.afnic.fr/fr/produits-et-services/services/zonecheck/

2 - Vulnérabilité CVE-2014-3466 affectant la bibliothèque GnuTLS

Contexte

Le CERT-FR a récemment publié l'avis de sécurité CERTFR-2014-AVI-248 au sujet d'une vulnérabilité affectant GnuTLS. Cette bibliothèque est une implémentation libre du protocole TLS (Transport Layer Security) qui permet la sécurisation des échanges de données sur Internet, analogue à la bibliothèque OpenSSL.

La faille décrite dans l'avis (CVE-2014-3466), dont souffre GnuTLS, est un dépassement de tampon dû à l'absence de validation d'un paramètre de taille reçu par un client TLS depuis un serveur. Cette faille entraîne une corruption de la mémoire au niveau du client, qui peut dans certains cas être exploitée pour parvenir à l'éxécution de code arbitraire.

Analyse de l'impact

Après l'attention légitime portée à la faille Heartbleed dans OpenSSL (CVE-2014-0160) en avril dernier, la présence d'une faille grave dans une autre implémentation du même protocole peut susciter une inquiétude particulière. Cependant, quelques différences majeures font que la faille de GnuTLS ne sera pas « le prochain Heartbleed ».

D'une part la faille de GnuTLS affecte les clients vulnérables, alors que Heartbleed affecte à la fois clients et serveurs TLS. Un seul serveur vulnérable à Heartbleed entraîne donc potentiellement la compromission de secrets concernant de multiples utilisateurs. En revanche l'exploitation de la faille GnuTLS repose sur la compromission préalable d'un serveur TLS pour rebondir ensuite vers des clients vulnérables, ou bien une première phase d'ingénierie sociale ou l'emploi d'une faille de type XSS pour attirer un client vulnérable vers un serveur malveillant. Dans un cas typique, si l'attaque sur le client fonctionne, un seul utilisateur est compromis.

D'autre part Heartbleed présente la particularité d'être trivialement exploitable de manière répétitive, et ce sans compromettre la stabilité d'un serveur visé, et par le biais d'une extension de protocole annexe dont l'usage n'est pas journalisé. L'exploitation à grande échelle de la faille GnuTLS nécessiterait un travail de développement d'un exploit stable. Cette issue n'est pas exclue mais les observations du CERT-FR indiquent une attention bien moindre portée par les attaquants potentiels à l'exploitation de cette faille, par rapport à Heartbleed, dans les quelques jours suivant sa découverte.

Enfin la diffusion de GnuTLS est moindre que celle d'OpenSSL. Parmi les clients les plus importants utilisant GnuTLS, on compte néanmoins les navigateurs Chromium et Iceweasel.

En résumé il s'agit donc d'une faille certes grave mais beaucoup moins critique que Heartbleed.

Recommandations

Le CERT-FR recommande de mettre à jour les systèmes affectés. Sous les systèmes Linux fondés sur Debian, il est possible de déterminer les paquetages dépendant de GnuTLS par le biais de la commande ci-dessous :

```
$ apt-rdepends -r libgnutls26
```

On peut aussi obtenir la liste des clients en cours d'exécution nécessitant d'être relancés par le biais de la commande :

```
$ lsof | grep gnutls
```

Documentation

- Avis CERTFR-2014-AVI-248 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-248/index.html
- Alerte Heartbleed :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-003/index.html

3 - Rappel des avis émis

Dans la période du 30 mai au 05 juin 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-247 : Vulnérabilité dans les produits VMWare
- CERTFR-2014-AVI-248 : Vulnérabilité dans GnuTLS
- CERTFR-2014-AVI-249 : Multiples vulnérabilités dans les produits F5
- CERTFR-2014-AVI-250 : Multiples vulnérabilités dans les produits F5
- CERTFR-2014-AVI-251 : Multiples vulnérabilités dans IBM Tivoli Monitoring
- CERTFR-2014-AVI-252 : Vulnérabilité dans Red Hat JBoss
- CERTFR-2014-AVI-253 : Multiples vulnérabilités dans OpenSSL

Gestion détaillée du document

06 juin 2014 version initiale.